6

06-1233 Oct. 30, 2006

No._____

In the
Supreme Court of the United States

EDDIE PAUL MUNOZ; PRO SE.
- Petitioner

v.

CENTRAL TELEPHONE COMPANY NEVADA; ET AL
-Respondents

On Petition for a Writ of Certiorari to the United States Court of Appeals for the 9th Circuit

APPENDIX U-V-W-X
VOLUME 5

EDDIE PAUL MUNOZ ; Pro Se
P.O. BOX 61344
LAS VEGAS, NEVADA 89160

APPENDIX U

PGS 270- 282

P.U.C. DOCKET.00-6057

BATES RECORD 010420 – 10438

F.C.C. SLAMMING INCIDENTS

TOLL FRAUD EXHIBIT

DOCUMENTED EVENT

INTERSTATE 800 NUMBERS

PREEMPTS FEDERAL JURISDICTION

Slamming Incidents

Trouble tickets incidents of slamming their were 4 incidences of slamming to another carrier MCI the importance of how devastated problem this is that it cuts off your billing which with 800 number. We pay for the usage payphone access etc. with the system that was set up had seventy eight 800 numbers 440-3500 thru 440-3599 100 DID numbers 24 PBX trunks which where supposed to be capability to hotel trunks which Sprint offers to business customers with end to end guarantees of trunking and fibers routes of hotels CEN reference this problem kept occurring this was not just one number we're talking about, 200 numbers that were slammed to the extent of having to put pic freeze on all numbers to keep them from being slammed these problems are very timely to a customer and costly due to lack of business and finding the problem and getting through this process do due to Sprint LD and local Sprint to work together. This stops all calls from coming in.

CEN 108 to 114
CEN 1464 to 1466
CEN 1543 to 1564
MUNOZ 000551-000552
MUNOZ 00304-000303-000296
CEN 1595
CEN 107 to 114
MUNOZ 000548 to 000556
MUNOZ 000560
MUNOZ 000566
MUNOZ 000335-000334
MUNOZ 000331-000326-000314-000307-000298-000297-000271-000270-000269-000268-000267-000266-000265
MUNOZ 000251-000167- to 000172
MUNOZ 000136-000135

Slamming

What you should know about Protecting you telephone service

State of Nevada
Public Utilities Commission

Carson City, Nevada
(775) 687-6000

Division of Consumer
Complaint Resolution

Las Vegas, Nevada
(702 486-2600

This page is best viewed at 800 x 600 resolutions

WHAT IS SLAMMING?

Slamming is the term used when your local or long distance carrier is illegally change without your consent

HOW CAN THIS HAPPEN

There are a number of ways unethical sales people can cause your phone service to be switched without your knowledge. The Federal Communications Commission allows companies to use telemarketing techniques to solicit your business. Telemarketers can cause your phone service to be switched by getting you to say "yes" during a telemarketing call. Also, you can inadvertently agree to switch your carrier by signing a card to enter a sweepstakes. In some circumstances, failure to return a postage-paid card within a certain number of days will trigger an unauthorized change. Sometimes a family member or office associate unknowingly authorizes the change.

HOW DO I KNOW I'VE BEEN SLAMMED?

Read your phone bill carefully each month. Make sure your local and long distance carriers are the ones you have chosen. Be familiar with the various charges and services. Also, you can call 1-700-555-4141 and a recording will tell you which long distance carrier is connected to your line.

If you are slammed, call your local phone company and request Primary Inter-exchange Carrier (PIC) protection on your phone line(s). A PIC freeze prohibits any change in long distance carriers without your express authorization.

Take preventive steps by educating your family and office associates. Only one person should have the authority to change your home or business phone company. Make sure everyone knows what to do if they receive calls regarding telephone service.

THE PUCN WILL HELP

The Public Utilities Commission of Nevada's Division of Consumer Complaint Resolution is here to help. In addition to tracking which companies are using misleading or fraudulent tactics, we can work with your long distance and local carriers to return you to your carrier of choice without any charge. We will work to obtain any refunds you are owed due to higher charges. Call us.
We have offices in Carson City (775) 687-6000; and Las Vegas (702) 486-2600.

DO ANY CONSUMER SAFEGUARDS EXIST?
Both the PUCN and FCC have rules that carriers should follow when soliciting a customer to switch phone companies. The rules say the customer is entitled to receive conformation of his requested switch in writing, by calling an 800 verification number and/or by having an independent third party verify the change. However, these consumer safeguards are increasingly being violated as

carriers compete for new customers in the competitive telecommunications markets.

WHAT IS CRAMMING?

Some companies also try to bill you for other calling services which you did not request. This practice is known as "cramming." The best defense is to listen carefully to sales pitches and closely review monthly bills. Whenever filling out sweepstakes entries, read the fine print.

WHAT ELSE CAN I DO?

You need to be a savvy phone customer. Ask questions. Never allow your service to be changed unless you fully understand the new rates and services you will be receiving. Sometimes there is a charge to switch phone companies. You need to know the amount of the charge and whether you or the new carrier will pay it.

Do not give out your credit card numbers, Social Security number, or other personal information over the phone to an unknown caller. Also, protect your Personal Identification Number (PIN) or any other personal information form an unknown caller.

You can also instruct a telemarketer to be put on the telemarketer's "do not call" list.

FINES/PENALTIES

Phone companies that break the rules and engage in illegal switching are subject to fines up to $100,000 per offense by the Federal Communications Commission. The FCC's toll free number is 1-888-225-5322.

They also can be prohibited from doing any business within Nevada. *If you've been slammed, we need to know.*

1.17.01		PUC	Rick Hackman		Meeting
1.18.01		3-Com	Arron Williams		Phone Call
1.24.01	2:33	Sprint	Doug	Slammed	Call regarding long distance
1.19.01		Amtec k	Tim, Jim	Meeting & Testing	Came to office to do test on phone lines
1.25.01		Sprint	Repair personal Patrick truck 825	Repair	Patrick Cichoshi Sprint Repair Truck liscence c820418 Truck 825 came to warehouse found bridge tap put in 1-400 100 200 count Order 145 Service 134 Transmitter brown and red.
1.25.01		Sprint			
1.26.01		Sprint Repair	Nathan	Slammed	Transferred call to Marty Class 71 Needed to call 800-880-8222 Complex repair long distance of 3 368 numbers
1.26.01		Sprint Compl ex Repair	Faye and Teresa		Given Ticket # WB01263768
1.27.01		Sprint Repair	Clint repair		Numbers were slammed to MCI long distance
1.29.01	2:37	Sprint	Scott		Called to reportrepair on lines and long distance change.
1.29.01		Sprint	Jerry		Slammed by

-					MCI
1.30.01		Sprint	Scott Collins	Phone Call	L.D. Cable, mail, Supervenes on TABS
1.30.01	2:11	OCB	Gayland	Phone Call	Doug 800-767-9406 10-10-333-702 slammed to MCI
1.31.01		OCB	Gayland		Natalin Riki Died
1.31.01	1:21	Sprint	Scott Collins	244-7172	Scott received fax I ask him about other lines going to facilities of t-1 line area
2.1.01	11:54	Sprint	Scott	Fax	Faxed to Scott 244-6497
2.2.01	4:00	Sprint	Scott Collins	Phone Call	Talked to Scott about the ling distance not working on 3 of the lines. He said he would get it fixed.
2.3.01	9:00	OCB	Gayland	Phone Call	Phone call to Gayland regarding what the new Hillsboro's phone girls had to say I.D. a switchman of Sprint robbery tape that goes to Hillsboro Enterprise 5030 Paradise Rd. office.
2.5.01		One Source	Segoria		Called to report Caller ID, *69 and consecutive roll over not working. she

					was out to lunch.
2.5.01	2:45	One Source	Segoria	Returned Phone Call	Stated it should be working needs someone at office to check the numbers
2.5.01	1:50		Kevin Poulsen	202-232-5200	Faxed testing report to 318-1112
2.6.01		Russ	Amtec		Order station win phone
2.6.01		Sprint	Scott Collins		Gave Scott information about (CODY) Rio incident
2.6.01		Sprint	Scott Collins		Lines on 3#s with MCI, Long distance back Kevin Poulsen will call him on security holes of Sprint
2.6.01	11:58	Amtec	Russ		Phone Call
2.6.01	11:00	OCB	Gayland		Phone Call Meeting after 6:30PM
2.6.01		Private Investi gator	Bert Goodrich		Phone Call
2.6.01	12:20		Kevin Poulsen		Phone Call
2.6.01	12:22	Sprint	Scott Collins		Left Message
2.7.01		Private Investi gator	Bert Goodrich	877-9149	Phone Call
2.7.01		Nevad a PUC	Ms Uttinger		Phone Call discussion RE: case 2 hour phone call
2.7.01	12:00	Nevad a PUC	Ms Uttinger		Phone Call
2.7.01	2:50	Attorn ey	Peter Alpert		Mrs. Uttinger called Mr. Alpert

2.7.01	3:00	Private Investi gator	Burt Goodrich		Phone Call
2.7.01			Kevin Poulsen		Left Word
2.7.01	4:03		Bobby Siller		Phone Call
2.7.01		Amtec	Jimmy	909-888-6932	Not until Monday
2.7.01		Nevad a PUC	Ms Uttinger		Fax
2.8.01			Kevin Poulsen		Kevin gave Lois Uttinger phone number
2.10.01			Kevin Poulsen		Phone call Kevin said he talked to PUC
2.10.01		OCB	Gayland		Phone sprint employees
2.10.01		Sprint Repair	Jody	888-862-8293 option 2	reported 368-6494 1-24-01 to Monica would call before noon given trouble ticket 165240
2.11.01	7:21	Sprint	Randy		Took off bridge tap last week
2.11.01	7:27				All lights lite up
2.12.01		Sprint Repair	John Parker and Randy T-one specialist		Ticket number 165240 closed reopen with New Ticket # 165674 T-1 spect switch problem signaling 457-5958 Scott Collins said circuit was nasty had to check transmission and switch. The ticket was closed before calling me.

(pages 2-8)

May-23-01 01:14pm From-BMO
7022444282 T-785 F-698
Datea=20102 User:uum990a 05/23/01

VIEW ALL REMARKS

UNABLE TO DIAL LONG DISTANCE FROM..
01/26/01 20:11 uum8372
LNS: 362-1364, 364-4873, 365-8873 & 367-7831.
GET TRAILOR OF 21H.
CONT. PEGGY OR ED @ 702-368-6494
ACC. 24HRS.
Opened arbs tkt 6224931 and referred to co dspch
01/26/01 22:47 h589221 for ca/pr test*****
THIS SUB HAS BEEN SLAMMED TO MCI. SHOULD
BE SPRINT 01/27/01 18:21 b667869
PLEASE CHG RCDS AND CHG IN SWITCH CHK W/
SUB FOR COMP INFO.
PLEASE CHANGE PIC BACK TO SPRINT, THEY
WILL NEED TO CALL BCAO MON AM TOLD
PEGGY WOULD CALL THE TA & SEE IF THEY CAN
CHANGE IT BACK 01/27/01 18:21 b667869
CALLED ON CALL TA TO CHANGE PIC BACK
Changed all pics to sprint**** 01/27/01 18:48 h589221

NEXT PREV DATE ADD UPDATE TOP BOTTOM
EXIT

May-23-01 01:14pm From-BMO
7022444282 T-785 F-698
Datea=1117 User:uum990a 05/23/01

SERVICE – ALL WORK ORDER DATA

Labor Price:	0.00	Labor Cost:	0.00
Part Price:	0.00	Part Cost:	0.00
Expenses:	0.00	Expense Cost:	0.00
Travel Price:	0.00	Travel Cost:	0.00
Flat Charge:	0.00	Type: Prm. CSR:	h589221
Start Milege:	0.00	Sec. CSR:	
Ending Mileage:	0.00	W.O. Paid?:	
Travel Time:	00.00	Restock Fee: 0.00	COD: no
Job Time:	0000:00	Job Number: Job Phase:	
Bill Time:	0000:00	Invoice: B013111798	
Bill Type:	3	Div: 776	
Customer PO:		Exempt: N	
P.M. Done:	N	Time Zone Number:	3
Tax Code: 290030080		Present Reading:	0.00
W.O. Class:		Last Reading:	0.00
Customer Code: 27781000		Cross Reference W.O.:	
Zip Code:	89119-1226	Territory: T-SOUTNV01	

NEXT-PAGE-Contract Information, PREV-PAGE-Return to the previous screen

SERVICE – ALL WORK ORDER DATA

W.O. Number: WB02274824 Site: 27781001
COMPUTER CONSULTING & DESIGN
Product Ref: Ent By: uuc732e Rem: Y
Serial Number: $2427781001001 Priority: 10 Hold: N
Model Number: ACCESS LINE W.O. Type: R3
Accepted: P
Caller: EDDIE MUNOZ Arr Tech Sup Date:
W.O. Phone: 702-368-6494 Leave Tech Sup Date:
Entry Date: 02/27/01 16:27
Dispatch Date: 02/27/01 16:27
Proj Arr Date: 02/28/01 15:27

Arrival Date: 02/28/01 15:27
Date Completed: 03/01/01 08:52
Cause: u Repair: ref Problem: 38
Subcontractor:
Retrofit:
Current Status: CI
Urgency Code: R
Premise Charge: 0.00
Action Group: wsaved Action Item:

NEXT-PAGE-Additional Information, F12-View Interrupts, F21- View Derts

May-23-01 01:14pm From-BMO
7022444282 T-785 F-698
Datea=20102 User:uum990a 05/23/01

VIEW ALL REMARKS

702-368-6494 AND 362-1366 UNABLE TO DIAL LONG. 02/27/01 18:32 uuc732e E
DISTANCE NUMBER EXAMPLE 775-372-5574. WAS TOLD BY SPRINT LONG DISTANCE TO CALL REPAIR CONTACT EDDIE MUNOZ @ 702-368-6494. ACCESS HOURS 24.
REPAIRED ACCESS LINE REPORTED BY EDDIE MUNOZ D
QUOTED TIME AND MATERIAL CHARGES TO EDDIE MUNOZ 02/27/01 18:33 uuc732e E
STATED HAVE A MAINTENANCE CONTRACT.
Opened arbs tkt 8232320 and referred to co dspch
02/27/01 23.20 h589221 E
for ca/pr test****
arbs ticket closed..ll
03/01/01 10:51 1724161 E
NEXT PREV DATE ADD UPDATE TOP BOTTOM EXIT

Task Name: 5182948
Customer Name: COMPUTER CONSULTING &
DESIGN SD: LNP: P
?Lead Task Nm:
Address: 4372 E. BOSTON AVE.
Phone Number: 702-368-6494
Billing Phone: 702-368-6494 Seq. Num: 0000001
Customer Type: B Circuit Num:
Status: ACT Out of Svc:N Orig OSS: N
Class of Svc: 71 Service Type: POTS
of Emps: 1 Report Categ: 1
?Skill: AUTO
Sub-Grid: 9N29 Maintenance: N
?Grid: E703
Access Code: Z Ticket Type: Appt Time:
Alarm Set: # of Repeats: 1
Tot Mins: 0 CTT Number:
#of Subseq: 0 Priorty Cd: 3
Due Date: 12/01/00 Due Time: 1845
Ver Code: Orig Due Date: 12/01/00
Orig Due Time: 1845 Test Date:
Log Date: 12/01/00 Log Time: 1101
Test Time: Party Pos: N Dev CD: 1Z
Essen Srv: N Adverse Comm?: Printer:0000
TROUBLE TICKET HISTORY
Lead Employee on this Trouble:
Dispatched To/ Trx Date/Trx Time/ Actual
Estimated
Dispatched-Updated by Duration

Proc	Status	Log Date	Log Time	Duration
PR	ACT	12/01/00	1102	0
0				1

UDS, UDS
Route Date: 12/01/00
PR ACT 11/30/00 1634 0
0
UDS, UDS
Route Date: 11/30/00

APPENDIX V

PGS-A- 283- 288

SECRET SERVICE CORRESPONDENCE

F.C.C. CORRESPONDENCE

SECURITIES EXCHANGE
COMMISSION WASHINGTON D.C.

UNITED STATES POSTAL SERVICE
First-Class Mail
Postage & Fees Paid
USPS Permit No. G-10

(Post Marked:
Las Vegas, NV 89014
23 May)

Sender: Please print your name, address, and ZIP+4 in this box

EDDIE PAUL MUNOZ
P.O. BOX 61344
Las Vegas, NV 89160

SENDER: COMPLETE THIS SECTION

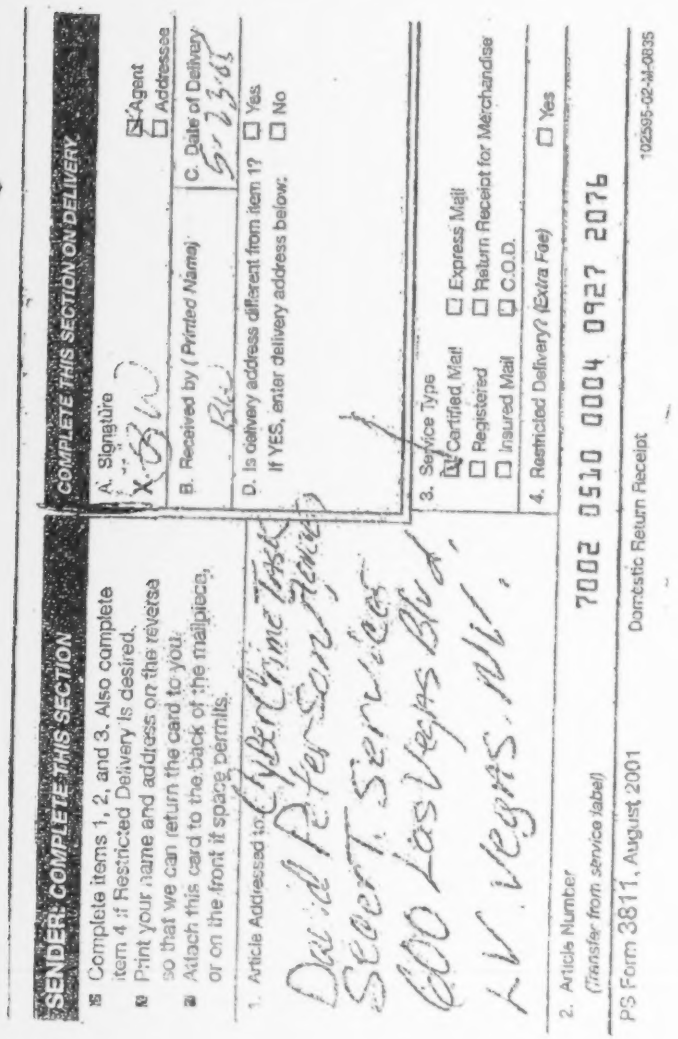
- Complete items 1,2, and 3. Also complete item 4 if Restricted Delivery is desired.
- Print your name address on the reverse so that we can return the card to you.
- Attach this card to the back of the mailpiece, or on the front if space permits.

1. Article Addressed to: Cyber Crime Task Force
   David Peterson
   Secret Service
   600 Las Vegas Blvd.
   Las Vegas, NV
2. Article Number: 7002 0510 0004 0927 2076
   (Transfer from service label)
3. Service Type
   *Certified Mail ☐Express Mail
   ☐Registered
   ☐Return Receipt for Merchandise
   ☐Insured Mail ☐C.O.D.
4. Restricted Delivery? (Extra Fee)

COMPLETE THIS SECTION ON DELIVERY

A. Signature: X (s) *Agent □Addressee
B. Received by (Printed Name): BW
C. Date of Delivery: 5-23-05
D. Is delivery address different from item 1? □ Yes
If YES, enter delivery address below: □ No

PS Form 3811, August 2001 Domestic Return Receipt
102595-02-M-0835



BEST AVAILABLE COPY

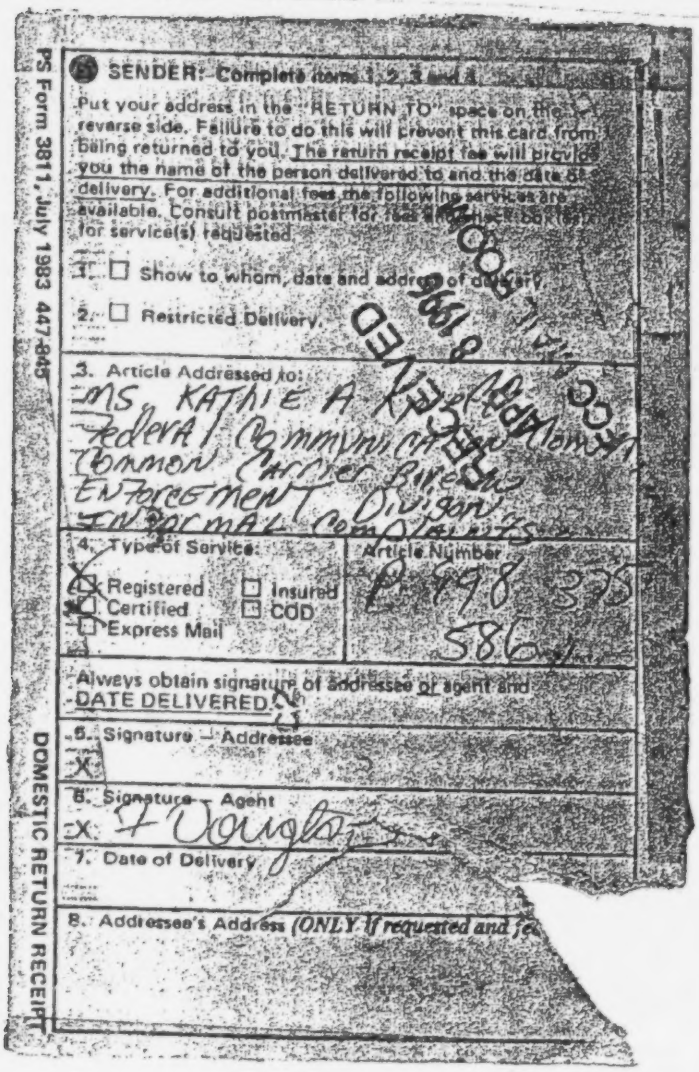
Thank You for your recent telephone inquiry regarding the status of your complaint about telecommunications common carrier service.

[ ] Your complaint File No. IC ____-_____ was received by the Consumer Protection Branch on _____. Pursuant to Section 208 of the Communications Act of 1934, the respondent carrier(s) has/have filed their response(s). The record is now being reviewed to identify possible violations the Communications Act, FCC Rules or Orders.

[ ] Your complaint, File No. IC ___-_____ has been served on the responsible carrier(s), and we are awaiting its/their response(s).

[X] Due to the high volume of complaints, your complaint has not yet been processed by the Consumer Protection Branch.

Thank you for contacting the Consumer Protection Branch.



PS Form 3811, July 1983 447-845

DOMESTIC RETURN RECEIPT

SENDER: Complete items 1, 2, 3 and 4.

Put your address in the "RETURN TO" space on the reverse side. Failure to do this will prevent this card from being returned to you. The return receipt fee will provide you the name of the person delivered to and the date of delivery. For additional fees the following services are available. Consult postmaster for fees and check box(es) for service(s) requested.

1. ☐ Show to whom, date and address of delivery.
2. ☐ Restricted Delivery.

3. Article Addressed to:
MS. KATHIE A KEHOE
Federal Communications
Common Carrier Bureau
Enforcement Division
Informal Complaints

4. Type of Service:
☒ Registered ☐ Insured
☒ Certified ☐ COD
☐ Express Mail

Article Number
P 798 335 586

Always obtain signature of addressee or agent and DATE DELIVERED.

5. Signature – Addressee
X

6. Signature – Agent
X F Douglas

7. Date of Delivery

8. Addressee's Address (ONLY if requested and fe

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
450 Fifth Street, NW
WASHINGTON, D.C. 20549-0213

August 3, 2002

Direct Dial (202) 942-7043
Office Of Investor Education And Assistance
Fax (202) 942-9634
E-Mail: SchockL@sec.gov
www.sec.gov

File No. HO 367907

Eddie Munoz
PO Box 61344
Las Vegas, NV 89160

Dear Mr. Munoz:

Thank you for your comments to the U.S. Securities and Exchange Commission concerning Sprint in Las Vegas. We welcome your comments because they help us to regulate and to enforce the laws that assure fair and orderly securities markets.

I have passed your views on to the people at the SEC who specialize in the issues you have raised. If they have any questions or wish to respond directly to your comments, they will contact you.

Once again, thank you for taking the time to inform us of your views.

Sincerely,
(s)_____
Lori J. Schock
Staff Attorney

APPENDIX W

PGS –A-289- 293

UNITED STATES SENATOR
HARRY REID

U.S. SENATOR
PUBLIC HEARING
APRIL 13 2006
5:30 PM

PUBLIC STATEMENT

SENATOR REQUEST

ENDER: COMPLETE THIS SECTION

Complete items 1, 2, and 3. Also complete item 4 if Restricted Delivery is desired.
Print your name and address on the reverse so that we can return the card to you.
Attach this card to the back of the mailpiece, or on the front if space permits.

Article Addressed to:

Fredo Rid.
FIT, Tom Breda.
333 LV Blvd.
Suite 8016
LV NV 89101,

COMPLETE THIS SECTION ON DELIVERY

A. Signature
X
☐ Agent
☐ Addressee

B. Received by (Printed Name) Luis Zaragoza
C. Date of Delivery

D. Is delivery address different from item 1? ☐ Yes
If YES, enter delivery address below: ☐ No

3. Service Type
☐ Certified Mail ☐ Express Mail
☐ Registered ☐ Return Receipt for Merchandise
☐ Insured Mail ☐ C.O.D.

4. Restricted Delivery? (Extra Fee) ☐ Yes

Article Number (Transfer from service label) 2026 4460 9000 0287 5002

Form 3811, February 2004 Domestic Return Receipt 102595-02-M-1540

United States Senate

WASHINGTON, DC 20510-2803

April 2006

Eddie Munoz
Strip Advertising
PO BOX 61344
Las Vegas, Nevada 89160

Dear Eddie:

I am honored to invite you to join me at an event with the Southern Nevada Chambers o Commerce on Thursday, April 13, 2006 at 5:30 pm. I will be addressing various issue facing the Southern Nevada economy, business community, and workforce. I look forward to hearing from you as a member of commerce on these and other important issues.

The Joint Chambers event will be held at the Clark Count Government Center Pyramid Building at 560 S. Grand Central Parkway in downtown Las Vegas.

Pleas RSVP to Tom Brede in my Las Vegas office as soon as possible by phone (702) 388-5020, fax (702) 388-5030, or e-mail tom_brede@reid.senat.gov. I look forward to seeing you there!

My best wishes to you.

Sincerely,

(s)_____

HARRY REID
United States Senator

STRIP ADVERTISING
P.O. BOX 61344
LAS VEGAS, NEVADA
89160

DEAR SENATOR REID,

HERE'S THE INFORMATION THAT YOU REQUESTED AT THE FORUM FOR THE BUSINESS COMMUNITY OF NEVADANS. IT IS HARD TO UNDERSTAND WHY? PEOPLE HAVE BEEN HIDING THESE ISSUES, FROM ONE OF ARE GREAT LEADERS, I HAVE BEEN FIGHTING THESE ISSUE'S SINCE 1991.
AND FOR ME SPEAKING ON THE TRUTH FOR ARE COMMUNITY AND STATE THE OF NEVADA. MY FAMILY'S BEEN HERE SINCE THE 50'S AND WE CAN'T RUN BACK HOME AND HIDE. FROM INLAND TERRORISTS, THAT ARE TAKING CONTROL OF OUR BUSINESS DAILY WHICH MAKE'S ME MADDER AND MADDER AT PEOPLE .THAT HIDE FROM THESE ISSUES BECAUSE THEY CAN'T STAND UP AND FIGHT FOR WHAT'S RIGHT HERE IN NEVADA. WE ARE AT WAR ,AND THE PEOPLE OF NEVADA NEED TO UNITE AND STAND UP AND BE AMERICAS. I THOUGHT THAT'S WHAT THIS GREAT NATION STOOD FOR, I HAVE LOST EVERYTHING MY FAMILY, MONEY AND INTEGRITY OVER THESE ISSUES THAT STAND BEFORE US. MY LIFE HAS BEEN IN DANGER FOR BRINGING THESE ISSUES TO THE LIGHT OF NEVADAN'S.
NEVADA'S BEEN MY HOME ALL MY LIFE AND AS OUR SENATOR, PLEASE HELP US THE BUSINESSES. NEVADA NEEDS, HELP WE CAN'T GET ANY HELP IN CYBER-CRIME DUE TO ENRON'S POLITICS. NOT WANTING TO ACKNOWLEDGE THAT IT EXISTS DUE TO THE DEPTH OF WAR ON OUR OWN HOME LAND TO

SAVE A BUCK AND PUT OUR CITIZEN'S AT RISK. CYBER-WAR IS HERE AND ARE SYSTEM'S ARE FAILING NEVADAN'S AND OUR BUSINESS'S.

THANK YOU SINCERELY,

EDDIE PAUL MUNOZ
(S)_____

APPENDIX X

PGS-A- 294-339

STATE OF NEVADA OFFICE
OF THE ATTORNEY GENERAL

CYBER CRIME NEVADA TASK FORCE

P.U.C. DOCKET 00-6057
BATES RECORD 010022-010028

DANIEL A MORRIS
ASSISTANT UNITED STATES ATTORNEY

COMPUTER AND TELECOMMUNICATIONS
COORDINATOR

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL

CYBER CRIME

- The Cyber Crime Task Force of Nevada Offers These Tips:
- Fighting Nevada High Technology Crime
- A Strategic Plan To Combat High Technology Crime
- Link to Criminal Justice Statistics Center
- Keeping You Child Safe on the Information Superhighway

For more information on the Cyber Crime Task Force of Nevada, visit their website:

CYBER CRIME
NEVADA TASK FORCE

http://ag.state.nv.us/hi_tech/home.htm 12/20/01

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL

HIGH TECH CRIME IS THE FASTEST GROWING THREAT IN THE AGE OF THE INTERNET – EVERY BUSINESS IS AT RISK. THE ATTORNEY GENERAL AND NEVADA'S HIGH TECH CRIME TASK FORCE OFFER THESE TIPS:

REVIEW SECURITY MEASURES:

1. Inventory and tag all equipment; keep operating manuals, warranties and proof of purchase. Have a reputable security specialist analyze your security procedures. Ask local law enforcement for their advice. If you hire security staff, provide them with adequate training.

2. Adopt written procedures for security and for the use of all high tech equipment including disposal of obsolete or broken equipment. Specify for what purposes the equipment may or may not be used, and whether the company is the owner of all work produced with company equipment.

3. High tech spies target insiders, repair persons, janitors, customers and consultants. Be cautious about divulging security information to others.

EMPLOYEES:

1. Conduct thorough background checks on all new employees, including temporary hires. Include criminal background checks where authorized by statute. Do not allow temporary staff access to sensitive data.

2. Train employees to be careful with sensitive data. Require that all waste documents be shredded.

3. Change passwords and locks when an employee is terminated or otherwise leaves your business.

4. Teach delivery staff techniques for avoiding cargo theft.

COMPUTERS:

1. Require employees to keep passwords confidential; change passwords frequently.

2. Periodic audits of company records should be conducted by a reputable service experienced in auditing computer accounts. Traditional accounting controls should not be abandoned when an office is computerized.

3. Require employees to back up their computers at least once per day. Adopt procedures for making hard copies of computer produced information. Secure backup tapes and diskettes.

4. Take steps to ensure that client information (financial, medical, legal or otherwise) is adequately secured.

5. Ensure that every computer operation can be handled by at least two employees.

6. Maintain adequate surge and anti-virus protection.

7. Remove all data from the hard drive before disposing of your old computer.

THE INTERNET:

1. Check the internet for your own product. This may help you uncover scams or false representations involving your product or service.

2. Don't keep banking or other confidential data on the same computer on which you have internet service.

3. Train employees regarding the hazards of divulging personal or confidential information on the internet.

4. Adopt written procedures for the use of internet services by employees.

TELECOMMUNICATIONS:

1. Establish procedures for the use of long distance service, cell phones, and other telecommunications equipment.

2. Verify the identity of people representing themselves as phone company technicians or repair persons by calling the company itself.

3. Be wary of delivery persons who ask to use your phone. Require that your staff place the call.

4. Train your staff to be on alert for "phone clones" and to report any unusual telephone activity or billings.

IDENTIFICATION:

1.Train employees to check credit card numbers and to compare information on the face of a credit card with the information printed out on the receipt.

2. Businesses which employ drivers should be alert for false drivers licenses and auto insurance certificates.

3. Develop a system for marketing or coding purchase orders, checks and other documents involving the financial transactions of your business so you will know of they are yours or are counterfeits.

4. Require fingerprints from customers presenting checks, money orders or traveler's checks.

GENERAL TIPS:

1. Be alert for suspicious behavior, such as the unexplained presence of persons in unauthorized areas.

2. If you observe anyone rummaging through garbage for papers, notify local law enforcement.

3. Adopt a "zero tolerance" approach toward high tech criminals. Prevent crime as best you can, but when it is detected, insist on pressing criminal charges and pursue all available civil remedies.

4. Knowing how your company's high tech equipment works will help you understand how to protect your business. Take any training which is offered at the time you purchase high tech equipment, read the manuals and get some "hands-on" experience with the new product.

5. Take any training which is offered at the time you purchase high tech equipment, read the manuals and get some "hands-on" experience with the new product.

A Message From Frankie Sue Del Papa

"Protecting your business from high tech crime does not have to be expensive or time consuming. The Office of the Attorney General and that University of Nevada Small Business Development Center have offered seminars to help small businesses learn from experts, and to teach law enforcement how to better prevent high tech criminals from stealing equipment, sabotaging or stealing customer and client information, charging long distance calls to business accounts, and using counterfeit checks and false identification to obtain products and services. Senate Bill 485 of the legislative session created the High Technology Crime Advisory Board which will be responsible for continuing the education of the business community and the general public."
If you are interested in assisting the Nevada High Technology Crime Task Force, a group of representatives from law enforcement and the business community working together to fight high tech crime, contact the Attorney General's Office (Kevin Higgins at 688-1818). Your suggestions, comments and ideas are welcome.

5/01
HIGH TECH CRIME
TIPS FOR BUSINESSES TO FIGHT HIGH TECH CRIME
NEVADA HIGH TECHNOLOGY CRIME TASK FORCE
OFFICE OF THE ATTORNEY GENERAL
Frankie Sue Del Papa Attorney General
100 N. Carson Street
Carson City, Nevada 89701-4717
(775) 687-4170

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

A Strategic Plan To Combat High Technology Crime In Nevada

CONTENTS

- Task Force Recommendations
- Executive Summary
- Members of Nevada's High Technology Crime Task Force
- Steering Committee Members
- Introduction
- Crimes Involving Computers and Components
- Computer Intrusion
- Telecommunications Fraud
- Technical Forensic Expertise and Assistance
- Prosecution Assistance

...to assist with the national endeavor against computer criminals. Efforts are also underway to enlist members of our country's computer industry to assist us in this fight and we are working towards getting a panel on this subject on the agenda for next year's COMDEX Convention in Las Vegas.

There are different ways you can help us in these efforts. If you or other members of your business can contribute expertise or equipment that would be of use to the task force, please contact Anne Cathcart of the Attorney General's Office at: (702) 687-3541.

The Task Force, in cooperation with the University of Nevada system, has planned a series of training seminars for businesses. These will be held beginning in February. For further information on participating in these seminars, please contact Kathy Carrico, State Training Director at the University of Nevada, Reno, at: (702) 784-1717.

The Attorney General's Office and the High Technology Task Force have developed a brochure with tips for businesses to help them combat high technology crimes. A copy of that brochure is included.

The involvement of the business community was identified by the task force as essential in helping to better equip law enforcement in their efforts to protect the community as a whole. Your suggestions, comments or ideas are needed, indeed, your participation is vital. Together, we can coordinate and share our resources to better fight the criminal elements in this new age of cyber crime.

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

EXECUTIVE SUMMARY OF TASK FORCE FINDINGS

Crimes involving computers and other high technology crime are the fastest growing criminal movement in the country. Computer crimes cost private industry between $5 billion and $10 billion annually. This number is expected to rise to $200 billion by the year 2000. Over $1 trillion is transferred every week by electronic wire. In the last five years technology theft has increased 323%. Only 1% of computer crime is being detected and only 7% of the detected crimes re reported to law enforcement. Of the cases which are detected and prosecuted, only 3% result in a jail sentence. Theft of long distance service is estimated at $3.7 billion a year. The average bank robber nets $2500, the average bank fraud nets $25,000 – the average computer crime nets $500,000 and the average theft of technology loss is $1.9 million.

Nevada's number one industry, gaming is a high tech industry which has and will continue to be a target for high technology crime. Cheating techniques often involve the use of high tech equipment and computer software, and may originate outside the state of Nevada.

Crimes are perpetrated against high technology manufacturers, retailers, businesses and homes containing computers and other equipment, and against anyone who makes cellular phone calls or who uses a credit card are common. High tech criminals forcibly take over warehouses and other businesses to steal computer equipment, hijack trucks, steal proprietary business information, perpetrate subscription fraud, cloning and toll

fraud against telecommunications companies and their customers, intrude into and disrupt corporate and government computers, pirate software, create false identification, counterfeit checks and other negotiable instruments and many other crimes. These crimes are committed against high tech targets or use high tech targets or use high tech means, or both.

The Nevada High Technology Crime Task Force was organized in July, 1997 at the direction of Attorney General Frankie Sue Del Papa and is compromised of representative of state, local and federal law enforcement agencies and private industry. The task force was created for the purpose of forming high technology crime units to conduct multi-jurisdictional investigations; track and disrupt the illicit commerce in stolen high tech goods, investigate and prosecute suspects engaged in white collar crime, organized crime and fraud against the government and private industry. The major goals of the task force are to:

- Investigate crimes involving computers and computer components, such as…

http://ag.state.nv.us/hi_tech/executive.htm 12/20/01

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

NEVADA HIGH TECHNOLOGY CRIME TASK FORCE RECOMMENDATIONS

The explosion of high tech crime, the loss of millions of dollars by industry and private citizens, and the danger to society as a whole posed by the high tech criminal mandate a response from law enforcement. The task force strongly recommends the immediate formation of high tech crime units and appropriate training for officers, prosecutors and judges. The task force makes the following specific recommendations:

- FORMATION OF TWO HIGH TECH CRIME UNITS, ONE IN NORTHERN NEVADA AND ONE IN CLARK COUNTY
- MANDATE AND PROVIDE HIGH TECH CRIME TRAINING FOR ALL NEVADA PEACE OFFICERS
- CERTIFY NEVADA LAW ENFORCEMENT OFFICERS IN COMPUTER FORENSIC ANALYSIS AND ASSIGN OFFICERS TO HIGH TECH CRIME UNITS
- EXECUTE MEMORANDA OF UNDERSTANDING BETWEEN ALL AGENCIES PARTICIPATING IN HIGH TECH CRIME UNITS
- PROVIDE BUSINESSES AND CITIZENS WITH EDUCATION IN PROTECTION AGAINST HIGH TECH TECH CRIME
- OBTAIN CONTINUED FUNDING AND SUPPORT FOR HIGH TECH CRIME UNITS

- NEVADA PARTICIPATION IN A WESTERN REGIONAL HIGH TECH CRIMES TASK FORCE
- PROVIDE HIGH TECH CRIME TRAINING TO PROSECUTORS AND JUDGES
- ENHANCE NEVADA LAWS RELATING TO HIGH TECH CRIME
- ESTABLISH STATEWIDE HIGH TECH CRIME DATABASE

http://ag.state.nv.us/hi_tech/recomend.htm 12/20/01

http://ag.state.nv.us/hi_tech/recommend.htm 12/20/01

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

MEMBERS OF NEVADA'S HIGH TECHNOLOGY CRIME TASK FORCE

(The following names were highlighted, taken from a much larger list)

Frankie Sue Del Papa, Attorney General
Alan Gallaspy, L.V. Metro
Steve Gibson, Esq., Lionel Sawyer & Collins
Kevin Higgins, Sr. DAG, A.G.'s Office
David Peterson, L.V. Metro
Bob Swiatek, Chief Inv., A.G.'s Office
David Vansant, FBI
Michael Taylor, Storey Co.
David Thompson, DAG, A.G.'s Office

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

STEERING COMMITTEE MEMBERSHIP

(The following names were highlighted, taken from a much larger list)

Lou Emmert, Sprint
Steve Franks, LVMPD
Jerry Kellar, Sheriff Clark County

State of Nevada -- Attorney General/Hi-Tech Crime/Plan 2

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

2. CRIMES INVOLVING COMPUTERS AND COMPONENTS.

Employee theft from manufacturers. When computer chips and components worth thousands of dollars can easily be hidden in an employee's pocket, some people cannot resist the opportunity to unjustly enrich themselves. These components are often untraceable and easily sold on the 'gray market' to less than honest manufacturers and retailers. We go to great lengths in the casino and mining industries in Nevada to prevent crimes of opportunity by employees, but is the same attention paid to the problem in our high tech industries? Such crimes should be prosecuted based on the value of the property stolen, which is oftentimes in the range of a major bank robbery. While employee theft is usually non-violent, it should not be relegated to the slap on the wrist associated with other white collar crimes.

Theft from computers at non-high tech businesses and institutions. The PC on a desk has become common place, but little though is given to securing this equipment from theft. But when an individual workstation and printer can be worth thousands, and the equipment in even a small office tens of thousands, businesses and public agencies become a preferred target for the high tech criminal. Most businesses and agencies have minimal after hours security, and simply by jimmying a door or breaking a window on late weekend night, a burglar can hit the jackpot. A retail store with an equal amount of inventory usually secures its goods at night, has an alarm system and is periodically checked by a security service. Most of

us unthinkingly leave essentials and extremely expensive equipment in an office in plain view from the street.

Fraud, counterfeiting and piracy. One of the biggest problems facing law enforcement is that many crimes are not even thought of as crimes by those who commit them. Does the average computer user think of copying someone else's software in the same way he thinks of shoplifting or petty theft? How many local businesses have proof of ownership for ever piece of software they are running? Microsoft recently sued several small computer manufacturers in the Bay Area for installing thousands of pirated copies of Windows on the PCs they sold. Failure to enforce the laws against software piracy only adds t5o the culture that creates users who do not think breaking into a computer system is a crime either. Another serious problem for the high tech industry is the counterfeiting of high tech products, including fake labels and equipment identification, and re-routing equipment by changing shipping labels.

Related crimes. The experience of the Sacramento Valley High Tech Crime Task Force is that the people and gangs involved in these new high tech crimes are also involved in many traditional crimes. Raids on high tech criminals have turned up piled of stolen and cloned cell phones as well as quantities of controlled substances and weapons. These new criminals seem to be following the business plan of the 90's and are diversifying their operations, incorporating high technology to assist them in carrying out traditional criminal activity with the added benefits of anonymity, no physical contact, and no significant financial investment.

Burglary and robbery at manufacturing sites, storage facilities and retail stores. Willie Sutton once said that the reason he robbed banks was because that's where the money was. The millions of dollars of components and equipment held by some computer manufacturers and other businesses has proven to be an irresistible target for

daylight invasion robberies by organized gangs. These robberies are often extremely violent and have resulted in the deaths of employees and bystanders. The proceeds can often be contained in a shoebox and are virtually untraceable. The same gangs are often implicated in telecommunications fraud, extortion, and drug sales and manufacturing. But their most profitable area is high tech theft, which is sure to be a growth industry in the next decade.

Cargo theft. High tech criminals employ various methods of hijacking expensive high tech cargo, especially that which is transported by trucking companies. One method, for example, is for one car to stop in front of the truck and another car drop directly behind the truck, making it impossible for the truck to go forward or backward. The car drivers then approach the truck driver with weapons. Truck drivers, including those employed by pickup and delivery services, are particularly vulnerable to being placed in physical danger in high tech cargo theft. The task force recommends that ruling companies provide instruction for their employees, to alert them to the various techniques of high-tech criminals. Procedures should also be established by trucking companies and associations to educate truck drivers so they can better protect themselves in at-risk situations.

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

3. COMPUTER INTRUSION.

In the movie War Games a teenage hacker brought the world to the brink of nuclear war. Today stories of hackers and the damage they cause are commonplace. Hackers break into business, private, and government computers to commit fraud, to destroy and alter records, and to simply create havoc. Hackers constantly change their methods and targets both to keep up with the changes in the high tech industry and to avoid detection. Businesses are sometimes blackmailed by hackers threatening to crash companies' file server, delete customer lists and customer e-mail, and corrupt databases.

While the specter of the teenager obsessed with computers working alone in his room at night is often the first image that comes to mind when thinking of computer intrusion, the more likely suspects are insiders, commonly greedy employees, or disgruntled former employees seeking vengeance. Who better knows how to break into your system and access sensitive information then the person who designed worked with it daily?

There are many basic measures a business can include in its procedures, such as changing passwords when an employee leaves, limiting access to high-level network functions, arranging for periodic audits, shredding its paper garbage, and many other steps, which can limit the possibility of crimes of opportunity.

One of the challenges facing the task force is that few businesses that are victims of computer intrusion report the crimes to law enforcement. Oftentimes there is a great

reluctance to let ones' customers, competitors o members of public know that the company's security has been compromised. May businesses would seem to prefer to absorb the loss in silence rather than risking the publicity which might accompany a prosecution. Unfortunately, this posture only serves to encourage high tech criminals.

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

4. TELECOMMUNICATIONS FRAUD

From the cloning of cell phones to the theft of calling cards to the slamming of long distance services, the average American is now the potential victim of a myriad of crimes that did not exist 20, 10 or even 5 years ago.

How do we begin to protect our citizens from crimes that can be committed without the criminal ever meting the victim face to face? The traditional law enforcement practice of having the victim or witnesses identify the perpetrator in front of a jury does not work for crimes committed by remote control.

By far the easiest way to deal with telecommunications fraud is to prevent it from happening. Deterrence is also a key element, but that works only of the criminal knows that similar cases have resulted in swift prosecutions and severe punishment.

Communications companies have begun to develop the ability to detect or prevent some types of criminal activity in the telecommunications area. For example, AT&T can disconnect cloned calls before the call is connected, because each phone has its own "fingerprint" which can be identified immediately upon placement of the call. AT&T's success with this phone print service has resulted in fewer phone cloning instances, but the service is not inexpensive.

Probably the most effective way to reduce telecommunications fraud is through the education of the public. Alerting users about the methods by which high

tech criminals attempt telecommunications fraud is essential for reducing such crimes as phone service subscription fraud. Both the telecommunications industry and the consumer must cooperate in the prevention and detection of these types of crimes.

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

5. TECHNICAL FORENSIC EXPERTISE AND ASSISTANCE

The investigation and prosecution of high tech crime present a special challenge to law enforcement. Law enforcement has fallen far behind the high tech criminal. Law enforcement officers have to learn such basic matters as what the primary components of a computer look like, how to secure the scene at computer crime (without inadvertently destroying evidence), how to handle high tech items and how to prevent suspects from erasing evidence right in front of them. Every line officer must be trained to recognize high tech equipment such as microprocessors, SIMMs, CD ROMs, mother boards, cloning devices and other evidence of high tech crime such as forged IDs and negotiable instruments. In the absence of this type of basic training, law enforcement will remain unable to respond effectively to high tech crime.

Officers must also be trained in the highly technical forensic analysis of computer software and hard drives. Officers must also understand the sophisticated technology used to commit high tech crime and must be certified computer forensic examiners in order to present evidence effectively in court.

This type of criminal activity is particularly complex and an officer handling computer crime needs a much lower caseload than other officers. It must also be noted that in order for a law enforcement agency to address high tech crime, officers must be dedicated full time.

The investigative complexity of these crimes requires painstaking and time-consuming analysis of crime scenes and seized evidence, and the creation of comprehensive profiles of high tech criminals. Establishing high tech forensic labs and databases is essential. It is a goal of the task force to assist Nevada law enforcement in overcoming these obstacles.

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

6. PROSECUTION ASSISTANCE.

Prosecutors and judges are similarly lacking in expertise and understanding of the technology utilized by the high tech criminal. High tech crime case law, although slowly evolving, is sparse and in many areas non-existent. The task force intends to provide ways to assist prosecutors and our courts in dealing with the high tech criminal.

In order to be able to present a high technology crime case to a jury, the prosecutor and the judge must have a fundamental understanding of the technical issues involved before they can hope explain them to someone else. By sponsoring training programs directed specifically at judges and prosecutors the task force can create a cadre of computer literate people who are ready to handle these complex cases.

It is recommended that programs for judges and lawyers be developed with the assistance of the National Judicial College, the Nevada Bar Association (Continuing Legal Education), the Nevada District Attorneys Association, and the newly formed Prosecution Advisory Council. The curriculum should include instruction on the preparation of lawful search warrants when high tech crime is involved; preservation of the evidence and establishing the chain of custody; qualifying and questioning expert witnesses in computer forensics; privacy and First Amendment issues; jury instructions in high tech crime cases; and the use of high tech demonstrative evidence.

Just as the task force recommends the dedication of law enforcement officers who receive training and acquire adequate experience to handle search and seizure situations, investigation techniques, and arrest in the high tech crime, the task force similarly recommends that there be at least one full-time prosecutor with training and experience in prosecuting high tech crime cases for each of the high tech crime units established in the state, one in the Las Vegas unit and one in the Reno/Sparks/Carson City area unit.

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

8. BUSINESS AND PUBLIC EDUCATION

Both private industry and the general public must be educated about high tech crime in order to defend against it. Simple techniques can be used to restrict access to computers and to prevent other intrusions (password changing, turning equipment off, maintaining confidentiality of social security numbers and other personal information). Businesses and individual's can be trained to identify pirated, cloned and stolen goods and to recognize forged instruments.

Private industry should also be familiar with high tech crime units and personnel, and be able to obtain appropriate assistance when needed. Many corporations offer toll-free numbers so consumers may check whether a specific piece of equipment was manufactured by the company, and if so, whether it has been reported as stolen. The establishment of two specific high tech crime units in northern and southern Nevada will make it easier for consumers and businesses to report suspected crimes.

A goal of the task force is to provide information to businesses and the general public, and to make training about high tech crime available. The task force is already working with the Small Business Development staff at the University of Nevada, Reno, on a series of seminars which will help owners and managers of small businesses in the community learn how to detect and prevent high tech crime. The task force intends to present similar seminars in southern Nevada. Law enforcement is assisting with similar educational efforts in Las Vegas. Requiring fingerprints on checks, conducting periodic audits of

internal functions, shredding paper documents, and thoroughly checking the references and background of job applicants- including temporary hires- are examples of measures that can be taken to reduce the potential for becoming a victim of high tech crime.

It is important to educate parents about criminal activity on the Internet, which could affect their children, including pornography and pedophilia. Teachers of computer science should be encouraged to include as part of their curriculum discussions on ethics and the law as they relate to high tech use. All Internet customers and especially vulnerable groups such as children, seniors, invalids, and the unsophisticated should be warned of consumer fraud activities on the Internet. Public education would include simple measures as changing the PIN number on a home answering machine; adequately checking on the legitimacy of any business advertising a product or business over the internet; refusing to be coerced into paying certain charges (usually by credit card) when you have been told you have "won" a prize or vacation; being aware of the potential dangers posed by "chat rooms", exercising caution about disseminating or discarding confidential personal data, etc.

The task force members recommend that a strong, cooperative effort to educate the public about high tech crime and its prevention should be initiated. In addition to seminars for business owners and managers, presentations can be made to parent groups and to students of all educational levels. Both corporate representatives and law enforcement officials a join in making public services announcements on television and radio. Brochures and other informational materials, including audio and visual aids, can be developed.

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

9. LEGISLATIVE CHANGES

As part of the effort to combat high tech crime, our laws must be strengthened. The task force recommends the following changes to the Nevada Revised Statutes be considered:

1. Impose stronger criminal penalties for high tech criminals, aiders and abettors, including restitution;

2. Allow businesses to obtain criminal background checks on prospective employees who will responsible for handling confidential data and financial data;

3. Expand definitions of high tech criminal activity to encompass newer forms of technology, which are developed;

4. Enhance ability of law enforcement to obtain search warrants in situations involving suspected high tech criminal activity;

5. Provide adequate resources for law enforcement to establish two high tech crime units in Nevada, including manpower, equipment and training;

6. Provide for strong civil penalties for high tech criminals, which will encourage victims of high tech crime to pursue civil remedies.

7. Work with other states to develop an interstate agreement, which can be enacted by all state legislatures to help eliminate jurisdictional problems.

Copies of current Nevada law related to computer and other high tech crimes are attached in Appendix A.

State of Nevada – Attorney General/Hi-Tech Crime/Plan 10

STATE OF NEVADA
OFFICE OF THE ATTORNEY GENERAL
Protecting Citizens, Solving Problems, Making Government Work

10. HIGH TECH CRIME UNITS/REGIONAL TASK FORCE

High tech crime units must be formed north and south in order to combat high tech crime. Without these units, law enforcement in Nevada will never effectively address high tech crime and will be powerless to respond to the multitude of criminal activity associated with high tech crime. The formation of these units is the primary and most important recommendation of the task force.

Task force members unanimously agree that the only way to combat high tech crime is through a coordinated multi-agency task force approach similar to the Sacramento High Tech Crimes Task Force. The Sacramento Task Force consists of twelve state, local and federal agencies with dedicated personnel and resources administered by the Sacramento County Sheriffs Office. The Sacramento Task Force has seven investigators who work high tech crimes on a full time basis. Other investigators participate part time on one to two shifts per week. The task force was created with the assistance of five comp0uter manufacturers and two cellular companies. Supporting businesses also provided furniture, office equipment, safety equipment, cash for informant fees, training and miscellaneous expenses The Sacramento Task Force works closely with the security departments of private companies, and cases are often directly forwarded from company6 security investigators to the task force.

In 1996 the Sacramento Task Force investigates property loss of more than $14 million and recovered more than $9 million. 156 suspects were arrested for illicit commerce in

components, burglaries, on line crimes, telecommunications fraud, financial fraud, gambling, robberies, narcotics and other offenses.
The task force recommends that two high tech crime units be formed in Nevada. One located in northern Nevada to provide assistance locally and to the rural counties, and one located in Clark County. The Office of the Attorney General will serve as a coordinating agency for the initiative against high tech crime and will also continue to provide prosecution assistance to the local entities as needed.

It is recommended that at a minimum, the following local, state and federal agencies should actively participate in the high tech crime units:

Northern Unit

Washoe County Sheriff
Washoe County District Attorney

Reno Police Department
Sparks Police Department
Nevada Attorney General
Nevada Division of Investigation
United States Attorney
FBI
Secret Service
US Postal Service

Southern Unit

Las Vegas Metropolitan Police
Clark County District Attorney
Las Vegas Police Department
Henderson Police Department
Nevada Attorney General
Nevada Division of Investigation
United States Attorney
FBI
Secret Service
US Postal Service

Corporate sponsors should also actively participate in the task force units.

In addition, the establishment of a Western States Regional High Tech Crime Task Force has been proposed to enable western states to enhance their efforts to combat high tech crime. Such a regional group could address issues concerning the multiple jurisdictional questions which arise in high tech crime; recommend legislation which will assist all affected law enforcement in the investigation and prosecution of high tech crimes; facilitate the consolidation and sharing of high tech resources among the western states; provide or coordinate

continuous opportunities for training which are cost-effective; and encourage and develop methods for law enforcement to share information regarding high tech criminal activity. The task force supports the concept of a regional entity.

Tracking a Computer Hacker

Daniel A. Morris
Assistant United States Attorney
Computer and Telecommunications Coordinator
District of Nebraska

A report written near the start of the Information Age warned that America's computers were at risk from hackers. It said that computers that "control [our] power delivery, communications, aviation and financial services [and] store vital information, from medical records to business plans, to criminal records, "were vulnerable from many sources, including deliberate attack. "The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb. "National Research Council, "Computers at Risk, "1991.

To see what computer hackers are doing today, look at www.attrition.org. This is one of the places on the Internet where hackers receive "credit" for their attacks. If the operator of this website verifies that a computer system has been invaded, a "mirror" of the damage, often a defaced web page, is posted on the website along with a link to the undamaged website. More importantly to the person or group claiming credit, the online nickname of the responsible hacker (HaXoBuGz, data boy and HACKWEISER being examples) is included next to the published description o the intrusion. This fleeting notoriety is what motivates many hackers. Other hackers cause even greater damage and try to avoid notice, much less notoriety.

Information about some of the Department of Justice's successes in prosecuting hackers can be found on the Department's website at www.cybercrime.gov. This site includes manuals for searching and seizing computers, policy statements, useful background material, and press releases regarding hacker prosecutions. It is one of the

first places prosecutors should go when called upon to assist investigators looking into computer intrusions.

Hacker Tools Available Online

Some websites on the Internet provide both novice and expert computer hackers with programs, sometimes called "exploits," needed to conduct attacks. These sites may provide services to computer security experts and eve advise hackers that they should not use the posted exploits to hack into another computer. Anybody, including some very destructive people, can download the hacker tools or "scripts" coded by experienced hackers, along with instructions for their use. See, e.g., http://www.securityfocus.com and its "bugtraq" service

Hackers who find exploits on these websites may use them to do more than just deface webpage's. Novices, sometimes referred to in hacker circles as "script-kiddies, "who download hacker scripts may gain "root" access to a computer system, giving them the same power over a computer system as a trusted systems manager – such as the power to create or delete files and e- mails and to modify security features.

Hackers who gain such unauthorized root access sometimes speak of this as "owning" the system they hack. If they want to cause damage they may do so immediately, or they may plant viruses or time bombs in a system. Sometimes they configure the system to work for them in later "denial of services: attacks on other computers.

Some websites that post hacker tools also post known fixes, or patches. They advise systems administrators and network operators to download and install these patches so their systems will no longer be vulnerable to the listed attacks. But hackers know that, with persistence and help from other readily available computer programs, they can find computer systems vulnerable to the listed exploits. Hackers frequently launch their attacks against these unprotected systems.

It is commonly believed that many systems operators do not share information when they are victimized by hackers. They don't contact law enforcement officers when their computer systems are invaded, preferring instead to fix the damage and take action to keep hackers from gaining access again—with as little public attention as possible.

Protected Computers

Federal law enforcement officers may be called in to track a hacker if the hacker gains unauthorized access to a Federal Government computer or to a computer system

protected by federal law. Protected computers are any computer used in interstate or foreign commerce or communications, which includes any computerco0nnecxted to the Internet. 18 U.S.C. & 1030 (e)(2)(B).

Tracking a hacker may call for a combination of Internet research skills, subpoenas, court orders, search warrants, electronic surveillance and traditional investigative techniques. At least one Assistant United States Attorney (AUSA) in every district has been trained as a Computer and Telecommunications Coordinator (CTC) to assist law enforcement officers and other AUSAs in this effort. CTCs can obtain guidance from attorneys in the Department of Justice's Computer Crimes and Intellectual Property Section (CCIPS) (pronounced See-sips). CCIPS attorneys deal with these issues daily.

Clues of a Cyber crime

A clue to the identity of a hacker often exist in cyberspace and in the real world of the investigator knows where to look.

Computer systems of interest to hackers usually keep track of all authorized and unauthorized access attempts. Records, called computer logs, provide useful and often critical clues that a trained agent or computer specialist can use as the starting point to trace the route taken from computer to computer through the worldwide web, to discover the one computer out of the millions in the world from which and intrusion was conducted.

All computers using the Internet are assigned a different numeric Internet Protocol (IP) address while online, similar to country, city, street, and number addresses for houses.
Unless the hacker alters the victim's logs once he or she gains unauthorized access, the victim'[s logs should list the precise computer address from which unauthorized

access was gained. That address may not be the hacker's own computer, but instead another computer that the hacker has hijacked or an account that he owns on a third party's computer, as discussed in more detail below.

Lookup tools are available online to identify the owner of the network through which an attack was launched. To see how this works, see www.arin.net. Operated by the American Registry of Internet Numbers.

Obstacles to Identifying the Hacker

Because of the make-up of the Internet, it is sometimes difficult for law enforcement officers to discover the identity of a hacker.

1. A hacker might hide or "spoof" his Internet Protocol (IP) address, or might intentionally bounce his communications through many intermediate computers scattered throughout the world before arriving at a target computer. The investigator must then identify all the bounce points to find the location of the hacker, but usually can only trace the hacker back one bounce point at a time. Subpoenas and court orders to each bounce point may be necessary to identify the hacker.

2. Some victims don't keep logs or don't discover a hacker's activities until it is too late to obtain records from the hacker's Internet Service Provider (ISP). A victim who has no record of the IP address of the computer from which unauthorized access was gained limits law enforcement officers to traditional investigative techniques, which alone may be inadequate to identify the hacker.

3. Some victims don't keep records or don't keep them long enough to be of help to law enforcement officers. As explained below, when the investigator determines the identity if an ISP from which records will be needed, the prosecutor should send a retention letter under 18 U.S.C.

& 2703 (f) requesting the ISP to preserve the records while a court order or other process is being obtained.

4. Some computer hackers alter the logs upon gaining unauthorized access, thereby hiding the evidence of their crimes.

5. Some leads go through foreign countries, not all of which consider hacking a crime. Treaties, conventions, and agreements are in place with some countries, and there are "24/7" contacts in dozens of countries around the world who can be contacted for help. When a lead points to a foreign country, the investigator should contact a CTC or CCIPS attorney.

Electronic Communications Privacy Act

Some of the information investigators need to track a hacker might be readily available to the general public on the Internet. No special restrictions apply to an investigator's access to and use of such information – in the same way that information available in a public library can be used by investigators without special authorization. Common search engines such as www.dogpile.com www.lycos.com www.excite.com or www.netscape.com may be used to find information about a username or nickname of the person or group claiming credit for a computer intrusion.

Other information, such as the content of e-mails, is available to law enforcement officers only if they comply with the provisions of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. && 2701-11. ECPA creates statutory rights for customers and subscribers of computer network service providers. The details of this Act are beyond the scope of this article, but an excellent guide to the Act is provided by CCIPS in print and on its webpage. See Computer Crime and Intellectual Property Section, Department of Justice, Prosecuting Intellectual Property Crimes Manual.

Section 2703 of ECPA provides investigators with five mechanisms for compelling an Internet Service Provider to disclose information that might be useful in an investigation of a hacker.

The mechanisms, in ascending order of the threshold showing required, are described below:

1. Subpoenas can be used by an investigator to obtain basic subscriber information from an Internet Service Provider, including "the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber or customer utilized. "U.S.C. & 2703(1)(C).

2. Subpoenas also can be used to obtain opened e-mails, but only under certain conditions relating to notice to the subscriber. See 18 U.S.C. & 2703(b)(1)(B). Notice may be delayed under Section 2705 for successive 90-day periods. Subpoenas may be issued for e-mails that have been opened, but a search warrant is generally needed for unopened e-mails.

3. Court orders under 18 U.S.C. & 2703(d) can be obtained by investigators for account logs and transactional records. Such orders are available if he agent can provide "articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an on going criminal investigation." Id.

The government must offer facts, rather than conclusory statements, in an application for a 2703 (d) order. A one to three-page factual summary usually is sufficient for this purpose. The standard for issuing such an order is not as high as for a search warrant.

4. Investigators who obtain a court order under 18 U.S.C. § 2703 (d) can obtain the full contents of a subscriber's account (except for unopened e-mail stored with an ISP for 180 days or less and voice-mail), if the order complies with a notice provision in the statute. 18 U.S.C. § 2703 (b)(1)(B)(ii) and (b)(2). Notice to the subscriber can be delayed for up to ninety days when notice would seriously jeopardize the investigation. 18 U.S.C. § 2705(a).

5. Search warrants obtained under rule 41 of the Federal Rules of Criminal Procedure or an equivalent state warrant can be used to obtain the full contents of an account, except for voice-mail in electronic storage (which requires a Title III order). The ECPA does not require notification to the subscriber when the government obtains information from a provider using a search warrant.

Warrants for information regarding evidence of a computer intrusion are usually obtained like all other search warrants but are served like subpoenas. That is, the agents serving the warrants on an ISP ordinarily do not search through the providers computers. Instead, they serve the warrants on the provider and the provider produces the material described in it.

Voluntary Disclosures

Investigators can obtain the contents of a hacker's communications stored on the victim system without first obtaining an order or a subpoena, pursuant to 18 U.S.C. § 2702(b). For example, a hacker's victim may voluntarily disclose the contents of internal e-mails relevant to the attack.

Voluntary disclosure by a provider whose services are available to the public is forbidden unless certain exceptions apply. These exceptions include disclosures "incident to the rendition of the service or the protection of the rights of property of the provider of the service or the protection of the rights of property of the provider of

the service." 18 U.S.C. § 2702(b)(5). See 18 U.S.C. §§ 2702 (b)(1)-(4), (6)(A)-(B) for other exceptions.

Early Communication with ISPs

Investigators should contact a network service provider as soon as possible to request that the ISP retain records that may be relevant to an investigation. This is often done through the AUSA who is assisting the agent in the investigation. The AUSA should send a letter to the ISP directing it to freeze stored records, communications, and other evidence pending the issuance of a court order or other process. 18 U.S.C. 2703 (f).

If the investigator wants to be sure the ISP does not disclose that the ISP has been asked for information pursuant to a subpoena, order or warrant, an order not to disclose can be obtained under 18 U.S.C. § 2705 (b).

Electronic Surveillance

Investigators tracking down hackers often want to monitor a hacker as he breaks into a victim's computer system. The two basic statues governing real-time electronic surveillance in other federal criminal investigations also apply in this context.

The first is the wire tap statute, 18 U.S.C. §§ 2510-22, generally known as a Title III order. The second statute relates to pen registers and trap and trace devices. 18 U.S.C. §§ 3121-27.

DOJ's manual for obtaining evidence of this type, says "In general, the Pen/Trap statute regulates the collection of addressing information for wire and electronic communications. Title III regulates the collection of actual content for wire and electronic communications." Computer Crime and Intellectual Property Section, Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal

Investigation 71 (2001) available at http://www.cybercrime.gov/searchmanual.pdf.

A warrant is suggested, at a minimum, when an investigator wants to obtain access to opened voice mail, but the requirements of Title III apply if the investigator wants access to voice mail messages not yet retrieved by a subscriber or customer.

Nationwide Scope of Tools Used in Hacker Investigations

18 U.S.C. § 2703 (d) orders are nationwide in scope, as are subpoenas. Other tools used in hacker investigations contain express geographic limitations. Search warrants under Fed.R.Crim.P. 41(a), Title III orders permitting the interception of communications, and 18 U.S.C. § 3123 (a) orders authorizing the installation of pen registers and trap and trace devices all apply only within the jurisdiction of the court.

Search Warrants

Search warrants may be obtained to gain access to the premises where the hacker is believed to have evidence of the crime. Such evidence would include the computer used to commit the crime, as well as the software used to gain unauthorized access and other evidence of the crime. Suggested language for a search warrant for evidence of this type is available in the online manual prepared by CCIPS.

Analyzing Evidence from a Hacker's Computer

A seized computer may be examined by a forensic computer examiner to determine what evidence of the crime exists on the computer. The court order should specifically authorize this search. Many federal agencies have trained personnel on staff who are able to prepare a mirror image of everything in the memory of a seized computer – often including the memory of things the

computer owner thought had been erased. The computer examiner will prepare a detailed report regarding the information on the computer and should be able to testify as an expert at trial.

The Use of Traditional Investigative Techniques

Information obtained through the methods described above may reveal the subscriber or customer whose computer was used to conduct an intrusion. If it does, traditional investigative techniques may then be needed to determine who actually used the identified computer to commit the crime.

Due to the anonymity provided by the Internet, a suspected hacker may claim that someone else used his computer and assumed his identity at the time of the attack. It may be difficult to prove otherwise. For example, In a case charged in the District of Nebraska, the identity of the suspected hacker who defaced a newspapers webpage by adding a bogus story was obtained even though computer logs showing the IP address of the hacker came to a dead-end because the hacker has used an ISP that provided anonymous access to the internet. United States v. Lynch, 8:00CR344 (D. Neb. Indictment filed Dec. 14, 2000). The now-defunct www.worldspy.com, kept no records of its users. Similar services still exist, such as www.anonymizer.com.

In the Nebraska case, calls to people in the community with the same last name as the person who was the subject of the unflattering article led authorities to the subject of the article, and that person led the FBI to the suspected hacker. Using tools available to obtain evidence of cyber crimes, including traditional investigative techniques such as this, federal law enforcement officer will continue to track down hackers and bring them to justice.

ABOUT THE AUTHOR

Daniel A. Morris is an Assistant United States Attorney (AUSA) in the District of Nebraska and is the Computer and Telecommunications Coordinator (CTC).

Mr. Morris has been an AUSA since 1987. Before that he was a Senior Corporate Counsel for the Mutual of Omaha Companies.

Mr. Morris is the author of two books, the Nebraska Trial Handbook and Federal Tort Claims, both published by West Publishing Company. Has published articles in the Creighton Law Review and for several years, was a regular contributor to Case and Comment, a magazine for lawyers.

Mr. Morris thanks CCIPS attorney Richard Dowing for his comments and suggestions regarding this article and also thanks Patrick DeWall, a law clerk for the District of Nebraska for his assistance.

Updated page July 10, 2001
Usdoj-crm/mis/jam